PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-083297

(43)Date of publication of application : 31.03.1998

(51)Int.Cl. G06F 9/06
G06F 12/14

(21)Application number : 09-120523

(22)Date of filing : 12.05.1997

(71)Applicant : FUJITSU LTD

(72)Inventor : AKIYAMA RYOTA
YOSHIOKA MAKOTO
UCHIDA YOSHIAKI

(30)Priority

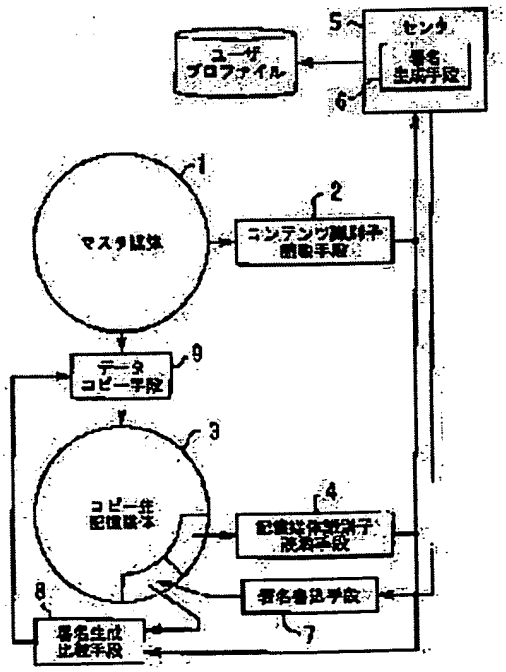
Priority number : 08124823 Priority date : 20.05.1996 Priority country : JP

(54) PROCESSOR AND METHOD FOR SOFTWARE COPY PROCESSING, AND COMPUTER-READABLE RECORDING MEDIUM WHERE PROGRAM FOR COPYING SOFTWRAE IS RECORDED

(57)Abstract:

PROBLEM TO BE SOLVED: To formally copy copyright protected software, stored on a master medium, to a user's storage medium as to the software copy processor.

SOLUTION: A content identifier read means 2 reads the identifier of software on the master medium 1 and a storage medium identifier read means 4 reads the identifier of the copy destination storage medium 3; and they are sent to a center 5 which administers copyright vending. The center 5 generates a signature from the information of the sent identifier by a signature generating means 6 and sends it to the user. The sent signature is written on the copy destination storage medium 3 by a signature write means 7. A signature generating and comparing means 8 generates a signature on the user side from the



information of the identifier sent to the center and compares this generated signature with the signature written on the copy destination storage medium 3 and only when the signatures match each other, a data copy means 9 reads the copy object software out of the master medium 1 and copies it to the copy destination storage medium 3.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－83297

(43)公開日　平成10年(1998)３月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ｇ
	12/14	３２０			12/14	３２０Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－120523

(22)出願日　平成９年(1997)５月12日

(31)優先権主張番号　特願平8－124823

(32)優先日　平８(1996)５月20日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　内田　好昭
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

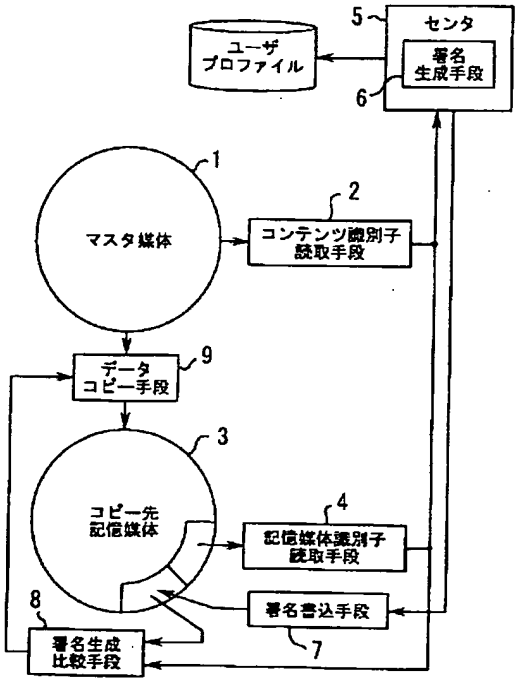
(74)代理人　弁理士　服部　毅巖

(54)【発明の名称】　ソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】　ソフトウェアコピー処理装置に関し、マスタ媒体に記憶された著作権保護ソフトウェアをユーザの記憶媒体に正当にコピーできるようにすることを目的とする。

【解決手段】　コンテンツ識別子読取手段２がマスタ媒体１上のソフトウェアの識別子を、記憶媒体識別子読取手段４がコピー先記憶媒体３の識別子をそれぞれ読み取り、コピー権販売を管理するセンタ５に送る。センタ５では署名生成手段６が送られた識別子の情報から署名を生成し、ユーザに送る。送られた署名は署名書込手段７によりコピー先記憶媒体３に書き込まれる。署名生成比較手段８はセンタに送った識別子の情報からユーザ側で署名を生成し、この生成した署名とコピー先記憶媒体３に書き込まれた署名とを比較し、署名が一致した場合のみ、データコピー手段９がマスタ媒体１のコピー対象ソフトウェアを読み出してコピー先記憶媒体３にコピーする。



【特許請求の範囲】

【請求項１】　マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理装置において、

個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第１の識別子の情報を読み取るコンテンツ識別子読取手段と、

コピー先記憶媒体毎に個別に記録された第２の識別子の情報を読み取る記憶媒体識別子読取手段と、

コピー権の販売を管理するセンタにおいて前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第１および第２の識別子の情報を受けてコピー対象ソフトウェアのコピー権を認証した第１の署名を生成する署名生成手段と、

前記署名生成手段において生成された前記第１の署名を前記コピー先記憶媒体に書き込む署名書込手段と、

前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第１および第２の識別子の情報から検証用の第２の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第１の署名を読み出して前記第２の署名と比較して一致するかどうかを判定する署名生成比較手段と、

前記署名生成比較手段における比較の結果、第１および第２の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段とを備えていることを特徴とするソフトウェアコピー処理装置。

【請求項２】　前記署名生成手段は、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第１および第２の識別子の情報をセンタが管理している認証鍵で暗号化した認証子を前記第１の署名として出力する署名処理手段と、前記署名処理手段で使用された認証鍵を前記センタに登録されているユーザ個別鍵で暗号化して前記認証子とともに出力する暗号化手段とを有していることを特徴とする請求項１記載のソフトウェアコピー処理装置。

【請求項３】　前記署名生成比較手段は、前記署名生成手段にて暗号化された認証鍵を前記センタに登録したユーザ個別鍵で復号して認証鍵を出力する復号手段と、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第１および第２の識別子の情報を前記復号手段が復号した認証鍵で暗号化して検証用の認証子を前記第２の署名として出力する認証子生成手段と、前記検証用の認証子と前記コピー先記憶媒体に第１の署名として書き込まれた認証子とを比較する比較手段とを有することを特徴とする請求項２記載のソフトウェアコピー処理装置。

【請求項４】　マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、

マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをコピー権要求情報と一緒にエンドユーザからコピー権を販売するセンタに送り、

前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタの認証鍵にて署名処理をして第１の認証子を生成するとともに前記認証鍵をユーザ個別鍵で暗号化処理して暗号化認証鍵を生成し、

生成された前記第１の認証子および暗号化認証鍵をエンドユーザに送り、

エンドユーザでは受けた前記第１の認証子および暗号化認証鍵を前記コピー先記憶媒体に書き込み、

前記コピー先記憶媒体に書き込まれた暗号化認証鍵をユーザ個別鍵で復号処理して前記センタで暗号化された認証鍵を取得し、

復号された認証鍵を使って前記コンテンツ識別子と記憶媒体識別子とを署名処理して検証用の第２の認証子を生成し、

生成された検証用の第２の認証子と前記コピー先記憶媒体に書き込まれた前記第１の認証子とを比較し、

前記コピー先記憶媒体に書き込まれた前記第１の認証子と前記検証用の第２の認証子とが一致した場合に、前記マスタ媒体のコピー対象データを読み出して前記コピー先記憶媒体に書き込む、

ことからなるソフトウェアコピー処理方法。

【請求項５】　マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理装置において、

個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第１の識別子の情報を読み取るコンテンツ識別子読取手段と、

コピー先記憶媒体毎に個別に記録された第２の識別子の情報を読み取る記憶媒体識別子読取手段と、

コピー権の販売を管理するセンタにおいて前記コンテンツ識別子読取手段が読み取った第１の識別子の情報から記憶媒体用変換鍵を生成するとともに前記記憶媒体識別子読取手段が読み取った第２の識別子の情報からマスタ媒体用変換鍵を生成し、生成した前記記憶媒体用変換鍵およびマスタ媒体用変換鍵を前記第２の識別子の情報で暗号化する変換鍵生成手段と、

前記変換鍵生成手段より出力された暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込む変換鍵書込手段と、

前記変換鍵生成手段より出力された暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記記憶媒体識別子読取手段が読み取った前記第２の識別子の情報で復号処理する変換鍵復号手段と、

前記マスタ媒体に記録されたコピー対象ソフトウェアを読み出し、前記変換鍵復号手段で復号された前記マスタ媒体用変換鍵で復号して平文のデータを出力するデータ

復号手段と、
前記平文のデータを前記変換鍵復号手段で復号された前記記憶媒体用変換鍵で暗号化して前記コピー先記憶媒体に書き込むデータ書込手段と、
を備えていることを特徴とするソフトウェアコピー処理装置。
【請求項６】　前記変換鍵生成手段は、前記コンテンツ識別子読取手段が読み取った第１の識別子の情報をセンタが管理しているマスタ鍵で暗号化して記憶媒体用変換鍵を生成する第１の暗号化手段と、前記記憶媒体識別子読取手段が読み取った第２の識別子の情報を前記マスタ鍵で暗号化してマスタ媒体用変換鍵を生成する第２の暗号化手段と、前記記憶媒体用変換鍵およびマスタ媒体用変換鍵を前記第２の識別子の情報で暗号化する第３の暗号化手段とを有することを特徴とする請求項５記載のソフトウェアコピー処理装置。
【請求項７】　ソフトウェアを識別するコンテンツ識別子とコピー権を販売するセンタが管理しているマスタ鍵とから作られたマスタ媒体用変換鍵によって暗号化されてマスタ媒体に記録されているソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、
マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをエンドユーザから前記センタに送り、
前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタのマスタ鍵で暗号化してマスタ媒体用変換鍵および記憶媒体用変換鍵を生成し、
前記マスタ媒体用変換鍵および記憶媒体用変換鍵をそれぞれ前記記憶媒体識別子で暗号化し、
暗号化された前記マスタ媒体用変換鍵および記憶媒体用変換鍵をエンドユーザに送り、
エンドユーザでは受けた暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込み、
受けた暗号化マスタ媒体用変換鍵および暗号化記憶媒体用変換鍵を前記記憶媒体識別子で復号し、
前記マスタ媒体のコピー対象データを前記マスタ媒体用変換鍵で復号して平文のデータにし、
前記平文のデータを前記記憶媒体用変換鍵で暗号化し、
暗号化されたデータを前記コピー先記憶媒体に書き込む、
ことからなるソフトウェアコピー処理方法。
【請求項８】　コンピュータを、
個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第１の識別子の情報を読み取るコンテンツ識別子読取手段、
コピー先記憶媒体毎に個別に記録された第２の識別子の情報を読み取る記憶媒体識別子読取手段、
前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第１および第２の識別子の情報をコピー権の販売を管理するセンタに送る送出手段、
前記第１および第２の識別子の情報から生成されたコピー対象ソフトウェアのコピー権を認証した第１の署名を前記センタから受け取る受信手段、
前記センタから受け取った前記第１の署名を前記コピー先記憶媒体に書き込む署名書込手段、
前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第１および第２の識別子の情報から検証用の第２の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第１の署名を読み出して前記第２の署名と比較して一致するかどうかを判定する署名生成比較手段、および前記署名生成比較手段における比較の結果、第１および第２の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項９】　コンピュータを、
個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第１の識別子の情報を読み取るコンテンツ識別子読取手段、
コピー先記憶媒体毎に個別に記録された第２の識別子の情報を読み取る記憶媒体識別子読取手段、
前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第１および第２の識別子の情報をコピー権の販売を管理するセンタに送る送出手段、
第１の識別子の情報から生成された記憶媒体用変換鍵および第２の識別子の情報から生成されたマスタ媒体用変換鍵を前記第２の識別子の情報で暗号化した暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記センタから受け取る受信手段、
前記暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込む変換鍵書込手段、
前記暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記記憶媒体識別子読取手段が読み取った前記第２の識別子の情報で復号処理する変換鍵復号手段、
前記マスタ媒体に記録されたコピー対象ソフトウェアを読み出し、前記変換鍵復号手段で復号された前記マスタ媒体用変換鍵で復号して平文のデータを出力するデータ復号手段、および前記平文のデータを前記変換鍵復号手段で復号された前記記憶媒体用変換鍵で暗号化して前記コピー先記憶媒体に書き込むデータ書込手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウ

ェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に著作権保護ソフトウェアをユーザの記憶媒体に正当にコピーするソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】近年、ソフトウェアの流通形態には様々のものがあり、フロッピーディスクやＣＤ－ＲＯＭ（ｃｏｍｐａｃｔ ｄｉｓｋ ｒｅａｄ ｏｎｌｙ ｍｅｍｏｒｙ）、半導体メモリなどの記憶媒体にソフトウェアを記録したものを購入したり、あるいはネットワークを経由してソフトウェアをダウンロードすることによって購入したりする場合があるが、これらのソフトウェアは通常いずれも他の記憶媒体に容易にコピーが可能なため、常に不正コピーの問題があり、著作権のあるソフトウェアについては深刻である。

【０００３】

【従来の技術】従来、コンピュータ用のアプリケーションプログラム、辞書データ、映像・音楽データなどのソフトウェアの販売形態の一つに、これらソフトウェアをＣＤ－ＲＯＭに電子的に鍵をかけた状態で記録して頒布する方法がある。この場合、ユーザは、そのソフトウェアの販売を管理しているセンタに連絡して利用したいソフトウェアの購入手続きをする。その後、ユーザは、購入手続き時に渡された鍵を使って鍵付きのソフトウェアを開くことにより、それをたとえばハードディスクにインストールすることができる。

【０００４】また、別の例として、書き込み可能な記憶媒体にあらかじめセンタが管理しているコピー権販売に関する識別子情報を書き込んでおく場合がある。ＣＤ－ＲＯＭに記録されたソフトウェアをコピーする場合は、その記憶媒体の販売店またはユーザがセンタに通知する。ソフトウェアの販売手続きをすることによってセンタから発行される識別子情報を記憶媒体に書き込まれた識別子情報と比較して一致する場合のみ、ＣＤ－ＲＯＭから記憶媒体にソフトウェアをコピーすることが可能になる。

【０００５】

【発明が解決しようとする課題】しかし、ハードディスクなどにインストールされたソフトウェアは、通常、そのまま実行あるいは利用できる、すなわち、鍵がかけられていないので、依然として不正コピーの問題は解消されていないという問題点があった。

【０００６】また、記憶媒体に識別子情報を書き込んでおく場合には、センタは記憶媒体を製造する工場と連携して識別子情報を管理する必要があり、しかも、記憶媒体についてコピー専用媒体と一般用記憶媒体とを区別して取り扱う必要があるという問題点があった。

【０００７】本発明はこのような点に鑑みてなされたものであり、マスタ媒体に記憶された著作権付きのソフトウェアをリード／ライト可能なユーザの媒体識別子付き記憶媒体に正当にコピーすることができるソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【０００８】

【課題を解決するための手段】図１は上記目的を達成する本発明の原理図である。本発明のソフトウェアコピー処理装置は、マスタ媒体１に記録されたコピー対象ソフトウェアの識別子を読み取るコンテンツ識別子読取手段２と、コピー先記憶媒体３の識別子を読み取る記憶媒体識別子読取手段４と、コピー権の販売を管理するセンタ５においてコンテンツ識別子読取手段２および記憶媒体識別子読取手段４が読み取った識別子の情報からコピー権を要求したユーザにコピー権を認証した署名を生成する署名生成手段６と、生成された署名をコピー先記憶媒体３に書き込む署名書込手段７と、コピー先記憶媒体３に書き込まれた署名とユーザ側で生成した署名とを比較する署名生成比較手段８と、比較結果が一致した場合にマスタ媒体１のコピー対象ソフトウェアをコピー先記憶媒体３にコピーするデータコピー手段９とから構成されている。

【０００９】上記の構成によれば、まず、コンテンツ識別子読取手段２がマスタ媒体１からソフトウェアのコンテンツ識別子を読み取り、記憶媒体識別子読取手段４がコピー先記憶媒体３からその記憶媒体識別子を読み取る。これらの識別子の情報は、センタに送られる。センタ５では、送られた識別子の情報から署名生成手段６が署名を生成してユーザに送り返す。その署名は、署名書込手段７によりコピー先記憶媒体３に書き込まれる。署名生成比較手段８は、コンテンツ識別子読取手段２および記憶媒体識別子読取手段４で読み取った識別子の情報から内部的に署名を生成してコピー先記憶媒体３に書き込まれた署名と比較する。この署名の比較が一致した場合は、データコピー手段９がマスタ媒体１から暗号化されたコピー対象ソフトウェアをそのままコピー先記憶媒体３にコピーする。

【００１０】また、本発明によれば、マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをコピー権要求情報と一緒にエンドユーザからコピー権を販売するセンタに送り、前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタの認証鍵にて署名処理をして第１の認証子を生成するとともに前記認証鍵をユーザ個別鍵で暗号化処理して暗号化認証鍵を生成し、生成された前記第１の認証子および暗号化認証鍵をエンドユーザに送り、エンドユーザでは受けた前記第１の認証子およ

び暗号化認証鍵を前記コピー先記憶媒体に書き込み、前記コピー先記憶媒体に書き込まれた暗号化認証鍵をユーザ個別鍵で復号処理して前記センタで暗号化された認証鍵を取得し、復号された認証鍵を使って前記コンテンツ識別子と記憶媒体識別子とを署名処理して検証用の第２の認証子を生成し、生成された検証用の第２の認証子と前記コピー先記憶媒体に書き込まれた前記第１の認証子とを比較し、前記コピー先記憶媒体に書き込まれた前記第１の認証子と前記検証用の第２の認証子とが一致した場合に、前記マスタ媒体のコピー対象データを読み出して前記コピー先記憶媒体に書き込む、ことからなるソフトウェアコピー処理方法が提供される。

【００１１】さらに、本発明によれば、コンピュータを、個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第１の識別子の情報を読み取るコンテンツ識別子読取手段、コピー先記憶媒体毎に個別に記録された第２の識別子の情報を読み取る記憶媒体識別子読取手段、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第１および第２の識別子の情報をコピー権の販売を管理するセンタに送る送出手段、前記第１および第２の識別子の情報から生成されたコピー対象ソフトウェアのコピー権を認証した第１の署名を前記センタから受け取る受信手段、前記センタから受け取った前記第１の署名を前記コピー先記憶媒体に書き込む署名書込手段、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第１および第２の識別子の情報から検証用の第２の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第１の署名を読み出して前記第２の署名と比較して一致するかどうかを判定する署名生成比較手段、および前記署名生成比較手段における比較の結果、第１および第２の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【００１２】この記録媒体は、好ましくは、ソフトウェアを記録しているマスタ媒体と同じ媒体とすることができる。コンピュータが記録媒体からコンテンツ識別子読取手段を読み出して実行することでマスタ媒体からソフトウェア個別の第１の識別子の情報が読み取られ、記憶媒体識別子読取手段４によりコピー先記憶媒体からコピー先記憶媒体毎に個別に記録された第２の識別子の情報が読み取られる。これらの識別子の情報は、送出手段によりコピー権の販売を管理するセンタに送られる。続いて、受信手段によりセンタからソフトウェアのコピー権を認証した第１の署名を受け取ると、署名書込手段がその第１の署名をコピー先記憶媒体に書き込む。次に、署名生成比較手段により、第１および第２の識別子の情報から内部的に第２の署名を生成してコピー先記憶媒体に書き込まれた第１の署名と比較し、これらの署名が一致した場合に、データコピー手段によりソフトウェアをマスタ媒体からコピー先記憶媒体にコピーする。

【００１３】

【発明の実施の形態】まず、本発明の概略について図面を参照して説明する。図１は本発明のソフトウェアコピー処理装置の原理構成を示す図である。

【００１４】この図において、本発明のソフトウェアコピー処理装置は、マスタ媒体１に記録されたコピー対象ソフトウェアのソフトウェア個別の識別情報を読み取るコンテンツ識別子読取手段２と、コピー先記憶媒体３の個別の識別情報を読み取る記憶媒体識別子読取手段４と、コピー権の販売を管理するセンタ５においてコンテンツ識別子読取手段２および記憶媒体識別子読取手段４がそれぞれ読み取った識別情報を受けてコピー対象ソフトウェアのコピー権を認証した署名を生成する署名生成手段６と、この署名生成手段６で生成された署名をコピー先記憶媒体３に書き込む署名書込手段７と、コンテンツ識別子読取手段２および記憶媒体識別子読取手段４がそれぞれ読み取った識別情報から署名を生成してこれとコピー先記憶媒体３に書き込まれた署名とを比較して一致するかどうかを判定する署名生成比較手段８と、この署名生成比較手段８にて署名が一致した場合にマスタ媒体１におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体３に書き込むデータコピー手段９とから構成されている。

【００１５】マスタ媒体１は販売対象のソフトウェアが暗号化されて記録されており、各ソフトウェアにはコンテンツ識別子が付けられている。また、コピー先記憶媒体３はその工場出荷時にあらかじめ個別の記憶媒体識別子が付けられているとする。ここで、ユーザがマスタ媒体１に記録されているソフトウェアの中からコピー対象ソフトウェアを指定すると、コンテンツ識別子読取手段２がマスタ媒体１からそのソフトウェアに対応するコンテンツ識別子を読み取り、記憶媒体識別子読取手段４がコピー先記憶媒体３からその記憶媒体識別子を読み取る。これら識別子の情報はコピー権購入の要求と一緒にセンタ５に送られる。センタ５では、署名生成手段６が受けたコンテンツ識別子および記憶媒体識別子の情報からコピー権を認証した署名を生成して、ユーザに送り返す。センタ５は、また、署名生成の際に、ユーザプロファイルに対してユーザの登録処理および課金処理を行う。

【００１６】ユーザ側では、署名書込手段７が署名生成手段６より送られて来た署名を受けて、これをコピー先記憶媒体３に書き込む。次いで、署名生成比較手段８においては、まず、コンテンツ識別子読取手段２により読み取られたコンテンツ識別子と記憶媒体識別子読取手段４により読み取られた記憶媒体識別子とから内部的に署名を生成し、次に、この生成された署名とコピー先記憶

媒体３に書き込まれた署名とを比較して一致しているかどうかを判定する。署名生成比較手段８における署名の比較が一致した場合は、データコピー手段９がマスタ媒体１から暗号化されているコピー対象ソフトウェアを読み取ってコピー先記憶媒体３に書き込む。ユーザがコピー先記憶媒体３に書き込まれたソフトウェアを利用する場合は、そのソフトウェアを復号しながらこのソフトウェアを実行する処理装置のメインメモリに展開して実行することになる。

【００１７】次に、本発明の実施の形態を、ＣＤ－ＲＯＭにて配付された著作権保護ソフトウェアをＭＯ（ｍａｇｎｅｔｏ－ｏｐｔｉｃａｌ　ｄｉｓｃ：光磁気ディスク）媒体にコピーする場合を例にして説明する。

【００１８】図２はソフトウェアコピー処理装置の処理の流れを示すフローチャートである。本発明のソフトウェアコピー処理装置において、ＣＤ－ＲＯＭに記録されたソフトウェアをＭＯ媒体にコピーする場合には、まず、エンドユーザ側にて、ＭＯ媒体の記憶媒体個別識別子ＩＤｋおよびＣＤ－ＲＯＭのコピーを希望するソフトウェアのソフトウェア個別識別子ＳＩＤｉを、コピー権の販売を管理しているセンタに送信する（ステップＳ１）。次いで、センタ側では、コピー権販売の手続き処理を行うとともに、受信された記憶媒体個別識別子ＩＤｋおよびソフトウェア個別識別子ＳＩＤｉから認証子ＣＳを生成してエンドユーザ側に送り返す（ステップＳ２）。エンドユーザ側では、受信した認証子ＣＳをＭＯ媒体の所定の記憶領域に書き込む（ステップＳ３）。ここで、エンドユーザ側においても、センタに送信した記憶媒体個別識別子ＩＤｋおよびソフトウェア個別識別子ＳＩＤｉを使って検証用の認証子ＣＳ′を生成する（ステップＳ４）。そして、エンドユーザ側で生成した認証子ＣＳ′とＭＯ媒体に書き込まれた認証子ＣＳとを比較する（ステップＳ５）。これら認証子ＣＳ′およびＣＳの比較の結果、両認証子が一致しているかどうかが判定され（ステップＳ６）、ここで、一致している場合には、ＣＤ－ＲＯＭからソフトウェア個別識別子ＳＩＤｉを有するソフトウェアの暗号化データをＭＯ媒体に書き込む（ステップＳ７）。もし、ステップＳ６に判定において、両認証子が一致していない場合には、ＣＤ－ＲＯＭからＭＯ媒体へのソフトウェアの書き込みは行われずに終了する。

【００１９】図３はＣＤ－ＲＯＭおよびＭＯ媒体の構成を示す図である。この図において、（Ａ）はＣＤ－ＲＯＭ１１の構成を示したもので、このＣＤ－ＲＯＭ１１には、それぞれソフトウェア個別識別子ＳＩＤｉ（ｉ＝１，２，・・・，ｎ）を有する著作権保護ソフトウェアと、ＣＤ－ＲＯＭからＭＯ媒体への著作権保護ソフトウェアのコピー操作を行うマネージャアプリケーションソフトウェアＭＡとが記録されている。各著作権保護ソフトウェアはそれぞれ暗号化された状態で記録されている。マネージャアプリケーションソフトウェアＭＡは、ＣＤ－ＲＯＭからＭＯ媒体へソフトウェアをコピーする場合に、エンドユーザ側のたとえばパーソナルコンピュータのような端末の本体に読み込まれて実行され、図２の処理のうちエンドユーザ側の処理を行う。

【００２０】また、（Ｂ）はＭＯ媒体１２の構成を示したもので、このＭＯ媒体１２には、記憶媒体個別識別子ＩＤｋ（ｋ＝１，２，・・・，ｍ）が記録されている。ＭＯ媒体１２はユーザが自由にデータを書き込んだり、消去することができる記憶領域を有しているが、ＭＯ媒体１２の記憶媒体個別識別子ＩＤｋが書き込まれている領域は、読み出しは可能であるが書き換えは不可能な領域である。この記憶媒体個別識別子ＩＤｋは、たとえば工場出荷時にそれぞれのＭＯ媒体に付けられるシリアル番号とすることができる。

【００２１】次に、ＣＤ－ＲＯＭの著作権保護ソフトウェアをＭＯ媒体にコピーする具体的な手順について説明する。図４は著作権保護ソフトウェアのコピー処理の手順を示す図である。

【００２２】この図において、コピー処理の手順を、たとえばパーソナルコンピュータで構成の本体側の処理とコピー権の販売を管理しているセンタ側の処理とに分けて示してあり、ここでは、本体側を〔エンドユーザ〕、センタ側を〔センタ〕で示し、それらの間は〔通信路／運搬路〕で示してある。

【００２３】ここで、エンドユーザの端末はＣＤ－ＲＯＭドライブ装置およびＭＯドライブ装置を備え、ＣＤ－ＲＯＭドライブ装置には、著作権保護ソフトウェアが記録されたマスタ媒体であるＣＤ－ＲＯＭ１１が装填されており、ＭＯドライブ装置にはコピー先の媒体であるＭＯ媒体１２が装填されているものとする。そして、ＣＤ－ＲＯＭ１１のコピー対象ソフトウェアはソフトウェア個別識別子ＳＩＤｉを有するソフトウェアであり、ＭＯ媒体１２に固有の識別子は記憶媒体個別識別子ＩＤｋであるとする。

【００２４】まず、エンドユーザの本体側処理では、ＣＤ－ＲＯＭ１１のマネージャアプリケーションソフトウェアＭＡを起動して、コピー対象ソフトウェアが指定されると、ＣＤ－ＲＯＭ１１からそのソフトウェアのソフトウェア個別識別子ＳＩＤｉが読み取られ、ＭＯ媒体１２から記憶媒体個別識別子ＩＤｋが読み取られる。これらソフトウェア個別識別子ＳＩＤｉおよび記憶媒体個別識別子ＩＤｋは、コピー権要求情報を含む要求文とともにセンタに送信される。

【００２５】センタ側では、受信したエンドユーザからの情報の要求内容をまず、ユーザプロファイル１３に書き込む。さらに、受信したソフトウェア個別識別子ＳＩＤｉおよび記憶媒体個別識別子ＩＤｋは署名処理装置１４に入力される。この署名処理装置１４は、秘密鍵であるセンタの認証鍵ＫＥＹｃを使ってデータ圧縮処理を行

い、認証子ＣＳを出力する。この認証子ＣＳが署名の役割を果たす。次に、署名処理装置１４で使用した認証鍵ＫＥＹｃは暗号化装置１５に入力され、ユーザ個別鍵ＫＵで暗号化されて、暗号化電文ＥＫＵ（ＫＥＹｃ）として出力される。署名処理装置１４より出力された認証子ＣＳおよび暗号化装置１５より出力された暗号化電文ＥＫＵ（ＫＥＹｃ）は、センタ識別子ＩＤｃとともにエンドユーザに送り返される。

【００２６】エンドユーザ側では、センタより送られた情報のうち、認証子ＣＳおよび暗号化電文ＥＫＵ（ＫＥＹｃ）はコピー先のＭＯ媒体１２上に一度書き込まれ、そしてこの書き込まれた媒体上の認証子ＣＳおよび暗号化電文ＥＫＵ（ＫＥＹｃ）がマネージャアプリケーションへ渡される。

【００２７】本体側処理では、署名検証のために、まず、渡された暗号化電文ＥＫＵ（ＫＥＹｃ）が復号装置１６に入力され、ユーザ個別鍵ＫＵを使用して復号されることにより、センタにおいて暗号化された認証鍵ＫＥＹｃが取り出される。次いで、署名処理装置１７において、ＣＤ－ＲＯＭ１１から読み取ったソフトウェア個別識別子ＳＩＤｉおよびＭＯ媒体１２から読み取った記憶媒体個別識別子ＩＤｋから、復号装置１６において復号された認証鍵ＫＥＹｃを使って、エンドユーザ側で検証用の認証子ＣＳ′を生成する。その後、ＭＯ媒体１２上に書き込まれた認証子ＣＳと署名処理装置１７で生成された認証子ＣＳ′とが比較器１８で比較される。比較器１８での比較の結果、認証子ＣＳと認証子ＣＳ′とが一致すれば、スイッチ１９が作動して、ソフトウェア個別識別子ＳＩＤｉを有するコピー対象ソフトウェアが暗号化データの状態で、コピー先のＭＯ媒体１２に書き込まれる。

【００２８】ここで、センタ側の署名処理装置１４およびエンドユーザ側の署名処理装置１７における処理の例について以下に説明する。図５は署名処理装置の構造例を示す図である。

【００２９】署名処理装置は、ソフトウェア個別識別子ＳＩＤｉおよび記憶媒体個別識別子ＩＤｋと認証子ＣＳとを受けて排他的論理和処理を行う排他的論理和処理部２１と、この排他的論理和処理部２１の出力とセンタの認証鍵ＫＥＹｃとを入力して認証子ＣＳを出力する暗号化処理部２２とからなり、ハッシュ関数を構成している。

【００３０】まず、入力されたソフトウェア個別識別子ＳＩＤｉおよび記憶媒体個別識別子ＩＤｋデータは、暗号化処理部２２においてブロック単位で認証鍵ＫＥＹｃにより暗号化される。暗号化処理部２２で暗号化処理された出力データは入力側に帰還されて、排他的論理和処理部２１において次のブロックデータと排他的論理和処理され、暗号化処理部２２で再び暗号化される。このような処理は、最終のブロックが入力されるまで繰り返される。この間、処理結果は出力されず、最終ブロックが暗号化されたとき、暗号化処理部２２から初めて認証子ＣＳとして出力される。

【００３１】次に、以上の手順でＭＯ媒体１２に暗号化されたままでコピーされたデータに含まれるソフトウェアのプログラムを実行する場合の処理手順について説明する。

【００３２】図６はコピーされたデータに含まれるソフトウェアのプログラムの実行処理手順を示す説明図である。ＭＯ媒体１２には、認証子ＣＳ、暗号化電文ＥＫＵ（ＫＥＹｃ）、記憶媒体個別識別子ＩＤｋデータ、およびソフトウェア個別識別子ＳＩＤｉが記録され、コピーされたソフトウェアは暗号化データＥＫｄ（ＤＡＴＡ）として記録されている。この暗号化データＥＫｄ（ＤＡＴＡ）はソフトウェアをＣＤ－ＲＯＭ１１に記録する際に鍵Ｋｄによって暗号化されたものであり、その暗号化に使用した鍵Ｋｄはマネージャアプリケーションソフトウェアによって保持されている。

【００３３】本体側処理では、まず、ＭＯ媒体１２から認証子ＣＳ、暗号化電文ＥＫＵ（ＫＥＹｃ）、記憶媒体個別識別子ＩＤｋデータ、およびソフトウェア個別識別子ＳＩＤｉが読み出され、その内の暗号化電文ＥＫＵ（ＫＥＹｃ）が復号装置１６に入力され、ユーザ個別鍵ＫＵを使用して復号されることで認証鍵ＫＥＹｃが取り出される。次いで、ＭＯ媒体１２から読み出したソフトウェア個別識別子ＳＩＤｉおよびＭＯ媒体１２から読み取った記憶媒体個別識別子ＩＤｋを、復号装置１６において復号された認証鍵ＫＥＹｃを使って、検証用の認証子ＣＳ′を生成する。その後、ＭＯ媒体１２上に書き込まれた認証子ＣＳと署名処理装置１７によって生成された認証子ＣＳ′とが比較器１８で比較される。比較器１８での比較の結果、認証子ＣＳと認証子ＣＳ′とが一致すれば、スイッチ１９が作動し、ＭＯ媒体１２から読み出された暗号化ソフトウェアである暗号化データＥＫｄ（ＤＡＴＡ）がそのスイッチ１９を経由して復号装置２５に入力される。復号装置２５では、入力された暗号化データＥＫｄ（ＤＡＴＡ）はマネージャアプリケーションソフトウェアが保持している鍵Ｋｄを使って復号され、平文のデータＤＡＴＡに戻される。このデータＤＡＴＡは、本体側の中央処理装置（ＣＰＵ）・メモリ２６のメモリ上にロードされ、ここで、そのソフトウェアのプログラムはＣＰＵによって実行処理される。

【００３４】次に、本発明のソフトウェアコピー処理装置の別の実施の形態について説明する。この例では、ＣＤ－ＲＯＭに記録されたソフトウェアはソフトウェア個別識別子ＤＩＤを有し、かつ、そのソフトウェアのデータＤａｔａはソフトウェア個別識別子ＤＩＤとコピー権販売センタが管理しているマスタ鍵ＫＭとから作られたマスタ媒体用変換鍵Ｋａによって暗号化され、暗号化データＥＫａ（Ｄａｔａ）になっているとし、ＭＯ媒体は

記憶媒体個別識別子Ｍｉｄのシリアル番号を有しているとする。

【００３５】図７はソフトウェアコピー処理装置の別のコピー処理の流れを示すフローチャートである。まず、エンドユーザ側にて、コピー先のＭＯ媒体の記憶媒体個別識別子ＭｉｄおよびＣＤ－ＲＯＭのコピーを希望するソフトウェアのソフトウェア個別識別子ＤＩＤをコピー権の販売を管理しているコピー権販売センタに送信する（ステップＳ１１）。次いで、センタ側では、受信されたソフトウェア個別識別子ＤＩＤがセンタに登録されているかどうかの検証が行われる（ステップＳ１２）。その後、受信された記憶媒体個別識別子Ｍｉｄおよびソフトウェア個別識別子ＤＩＤをセンタ管理のマスタ鍵ＫＭで暗号化して記憶媒体用変換鍵ＫｕおよびマスタＭ媒体用変換鍵Ｋａを生成する（ステップＳ１３）。次いで、これら記憶媒体用変換鍵ＫｕおよびマスタＭ媒体用変換鍵Ｋａを記憶媒体個別識別子Ｍｉｄで暗号化して暗号化電文ＥＭｉｄ（Ｋｕ，Ｋａ）を生成し、生成した暗号化電文ＥＭｉｄ（Ｋｕ，Ｋａ）を要求元のエンドユーザへ送り返す（ステップＳ１４）。エンドユーザ側では、受信した暗号化電文ＥＭｉｄ（Ｋｕ，Ｋａ）のうち、ＭＯ媒体に関連した情報を有する暗号化電文ＥＭｉｄ（Ｋｕ）をＭＯ媒体に書き込むとともに受信した暗号化電文ＥＭｉｄ（Ｋｕ，Ｋａ）を記憶媒体個別識別子Ｍｉｄで復号して記憶媒体用変換鍵ＫｕおよびマスタＭ媒体用変換鍵Ｋａを得る（ステップＳ１５）。次に、ステップＳ１５で得られたマスタＭ媒体用変換鍵Ｋａを使用して、ＣＤ－ＲＯＭのソフトウェア個別識別子ＤＩＤに対応する暗号化データＥＫａ（Ｄａｔａ）を復号し、平文のデータＤａｔａを得る（ステップＳ１６）。そして、このデータＤａｔａをステップＳ１５で得られた記憶媒体用変換鍵Ｋｕで再暗号化してＭＯ媒体に書き込み、コピーを終了する（ステップＳ１７）。

【００３６】次に、ＣＤ－ＲＯＭのソフトウェアをＭＯ媒体にコピーする具体的な手順について説明する。なお、エンドユーザ側でコピー権販売センタに要求を出すときに最初に行われる処理は、コピー先のＭＯ媒体の記憶媒体個別識別子ＭｉｄおよびＣＤ－ＲＯＭのコピー対象ソフトウェアのソフトウェア個別識別子ＤＩＤの読み出し処理と、これら記憶媒体個別識別子Ｍｉｄおよびソフトウェア個別識別子ＤＩＤのセンタへの送信処理だけなので、この最初の処理に関する説明は省略し、センタ側の処理の説明から行う。

【００３７】図８はセンタ側における処理の手順を示す説明図である。この図において、センタは、まず、回線を通じてエンドユーザから送信された記憶媒体個別識別子Ｍｉｄおよびソフトウェア個別識別子ＤＩＤを受信し、このうち、記憶媒体個別識別子Ｍｉｄをセンタ管理のマスタ鍵ＫＭを有する暗号化装置３１に入力し、ソフトウェア個別識別子ＤＩＤを比較器３２へ入力する。暗号化装置３１は記憶媒体個別識別子Ｍｉｄをマスタ鍵ＫＭで暗号化して記憶媒体用変換鍵Ｋｕを生成する。一方、比較器３２は、ソフトウェア個別識別子ＤＩＤの正当性検証のため、発行コンテンツ識別子ファイル３３を検索し、要求されたソフトウェア個別識別子ＤＩＤと比較する。ここで、発行コンテンツ識別子ファイル３３のソフトウェア個別識別子ＤＩＤと要求されたソフトウェア個別識別子ＤＩＤとが一致した場合には、スイッチ３４は閉成状態に制御される。すると、要求されたソフトウェア個別識別子ＤＩＤはマスタ鍵ＫＭを有する暗号化装置３５に入力される。暗号化装置３５はソフトウェア個別識別子ＤＩＤをマスタ鍵ＫＭで暗号化してマスタ媒体用変換鍵Ｋａを生成する。暗号化装置３１で生成された記憶媒体用変換鍵Ｋｕおよび暗号化装置３５で生成されたマスタ媒体用変換鍵Ｋａは暗号化装置３６に入力され、それぞれ記憶媒体個別識別子Ｍｉｄによって暗号化される。暗号化装置３６によって暗号化された暗号化電文ＥＭｉｄ（Ｋｕ，Ｋａ）は回線を通じて要求元のエンドユーザに送信される。この処理が達成されると、ユーザプロファイル３７に課金処理の指示が伝えられ、要求元のエンドユーザに対して課金が実施される。

【００３８】図９はエンドユーザ側における処理の手順を示す説明図である。この図において、センタから送信された暗号化電文ＥＭｉｄ（Ｋｕ，Ｋａ）を受信すると、まず、そのうちのＭＯ媒体に関する暗号化電文ＥＭｉｄ（Ｋｕ）をＭＯ媒体４０の所定の領域４１に書き込む。そして、受信された暗号化電文ＥＭｉｄ（Ｋｕ，Ｋａ）は復号装置５１に入力される。復号装置５１はＭＯ媒体４０の記憶媒体個別識別子Ｍｉｄを使って暗号化電文ＥＭｉｄ（Ｋｕ，Ｋａ）を復号し、記憶媒体用変換鍵ＫｕおよびマスタＭ媒体用変換鍵Ｋａを出力する。復号されたマスタＭ媒体用変換鍵Ｋａは復号装置５２に復号鍵として入力され、記憶媒体用変換鍵Ｋｕは暗号化装置５３に暗号鍵として入力される。まず、復号装置５２は、ＣＤ－ＲＯＭ６０のソフトウェア個別識別子ＤＩＤに対応する暗号化データＥＫａ（Ｄａｔａ）を読み込んでマスタ媒体用変換鍵Ｋａにより復号し、平文のデータＤａｔａに戻して出力する。このデータＤａｔａは暗号化装置５３に入力され、記憶媒体用変換鍵Ｋｕで再暗号化される。暗号化装置５３で暗号化された暗号化データＥＫｕ（Ｄａｔａ）はＭＯ媒体４０に書き込まれる。

【００３９】次に、以上の手順でＭＯ媒体４０に書き込まれた、このＭＯ媒体４０に固有の識別子およびセンタのマスタ鍵に基づく変換鍵による暗号化データＥＫｕ（Ｄａｔａ）を利用する場合の処理手順について説明する。

【００４０】図１０はコピーされたデータの利用処理手順を示す説明図である。ＭＯ媒体４０は、書き換え可能な領域の中の領域４１に暗号化電文ＥＭｉｄ（Ｋｕ）が記憶され、書き換え不可能な領域４２に記憶媒体個別識

別子Ｍｉｄが記憶され、それ以外の領域の一部にコピーされた暗号化データＥＫｕ（Ｄａｔａ）が記憶されている。ここで、暗号化データＥＫｕ（Ｄａｔａ）を利用する場合は、まず、ＭＯ媒体４０上の記憶媒体個別識別子Ｍｉｄおよび暗号化電文ＥＭｉｄ（Ｋｕ）が読み出されて復号装置５４に入力される。復号装置５４は記憶媒体個別識別子Ｍｉｄを用いて暗号化電文ＥＭｉｄ（Ｋｕ）を復号し、記憶媒体用変換鍵Ｋｕを出力する。復号装置５５は記憶媒体用変換鍵Ｋｕを復号鍵として使用し、ＭＯ媒体４０から読み出された暗号化データＥＫｕ（Ｄａｔａ）を復号して、平文のデータＤａｔａを出力する。このデータＤａｔａはエンドユーザの端末であるパーソナルコンピュータのメインメモリ上に展開され、これがプログラムならば実行され、辞書データならば検索するなどして利用される。

【００４１】

【発明の効果】以上説明したように本発明では、マスタ媒体のコピー対象データの識別子およびコピー先記憶媒体の識別子の情報から署名を生成する署名生成手段をセンタ側に備え、エンドユーザ側では署名生成手段によって生成された署名をコピー先記憶媒体に書き込む署名書込手段と、エンドユーザ側で生成した検証用の署名とコピー先記憶媒体に書き込まれた署名とを比較する署名生成比較手段と、比較結果によってマスタ媒体のコピー対象データをコピー先記憶媒体に書き込むデータコピー手段を備えるように構成した。このため、センタは、コピー先記憶媒体の識別子の情報に対してこれと対応する署名を発行するだけでよく、また、コピー先記憶媒体の製造工場と連携しての識別子情報の管理というようなことも必要なく、コピー先記憶媒体を製造する工場やこれを販売する店において、コピー先記憶媒体の在庫管理を不要にすることができる。

【図面の簡単な説明】

【図１】本発明のソフトウェアコピー処理装置の原理構成を示す図である。

【図２】ソフトウェアコピー処理装置の処理の流れを示すフローチャートである。

【図３】ＣＤ－ＲＯＭおよびＭＯ媒体の構成を示す図である。

【図４】著作権保護ソフトウェアのコピー処理の手順を示す図である。

【図５】署名処理装置の構造例を示す図である。

【図６】コピーされたデータに含まれるソフトウェアのプログラムの実行処理手順を示す説明図である。

【図７】ソフトウェアコピー処理装置の別のコピー処理の流れを示すフローチャートである。

【図８】センタ側における処理の手順を示す説明図である。

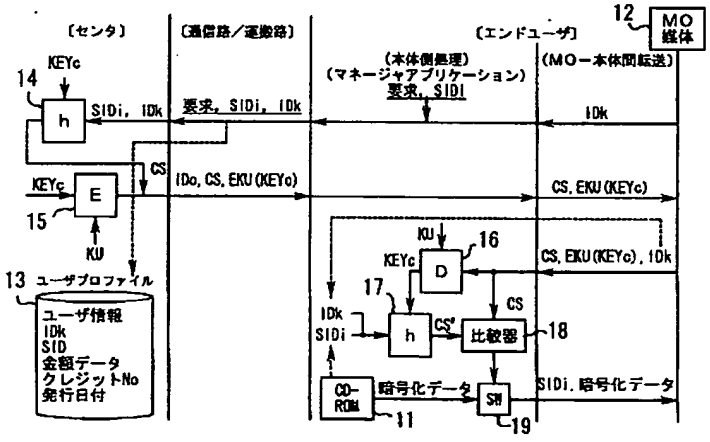
【図９】エンドユーザ側における処理の手順を示す説明図である。

【図１０】コピーされたデータの利用処理手順を示す説明図である。

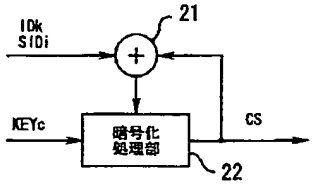
【符号の説明】

1　マスタ媒体
2　コンテンツ識別子読取手段
3　コピー先記憶媒体
4　記憶媒体識別子読取手段
5　センタ
6　署名生成手段
7　署名書込手段
8　署名生成比較手段
9　データコピー手段

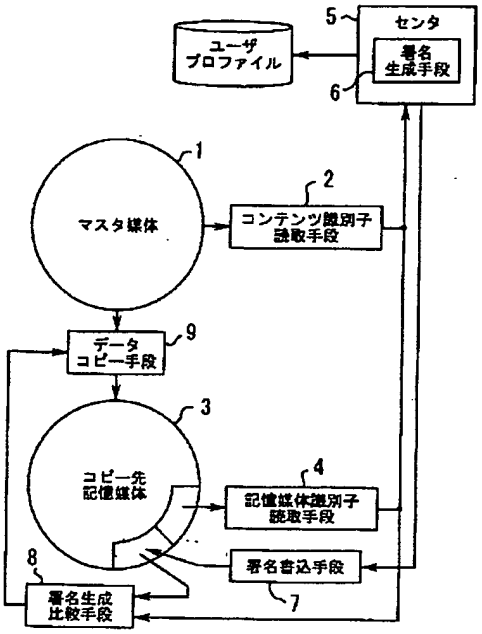
【図４】



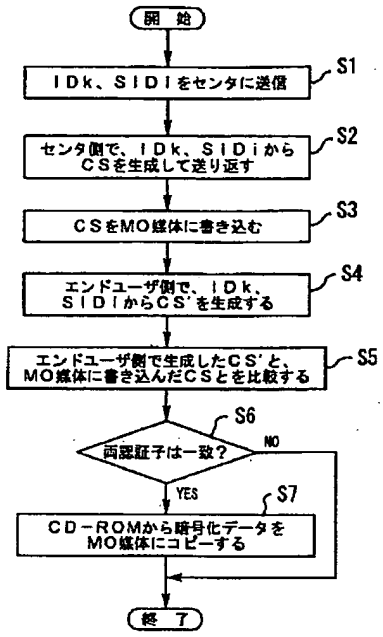
【図５】



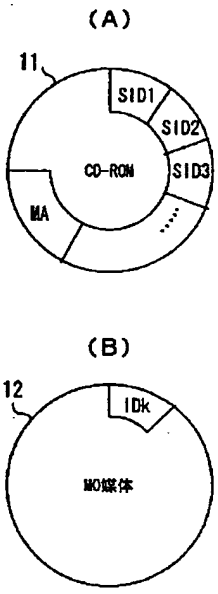
【図1】



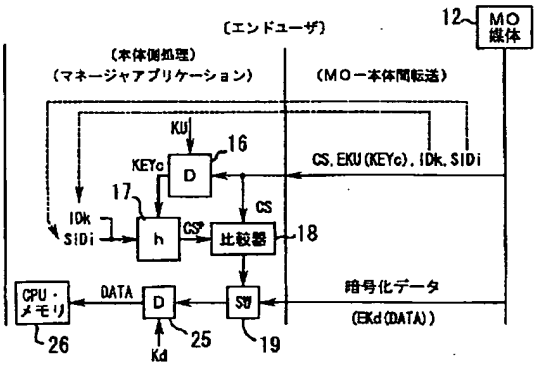
【図2】



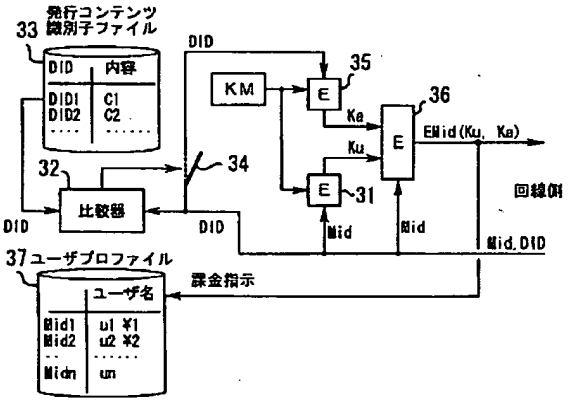
【図3】



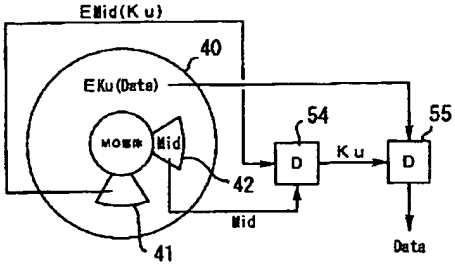
【図6】



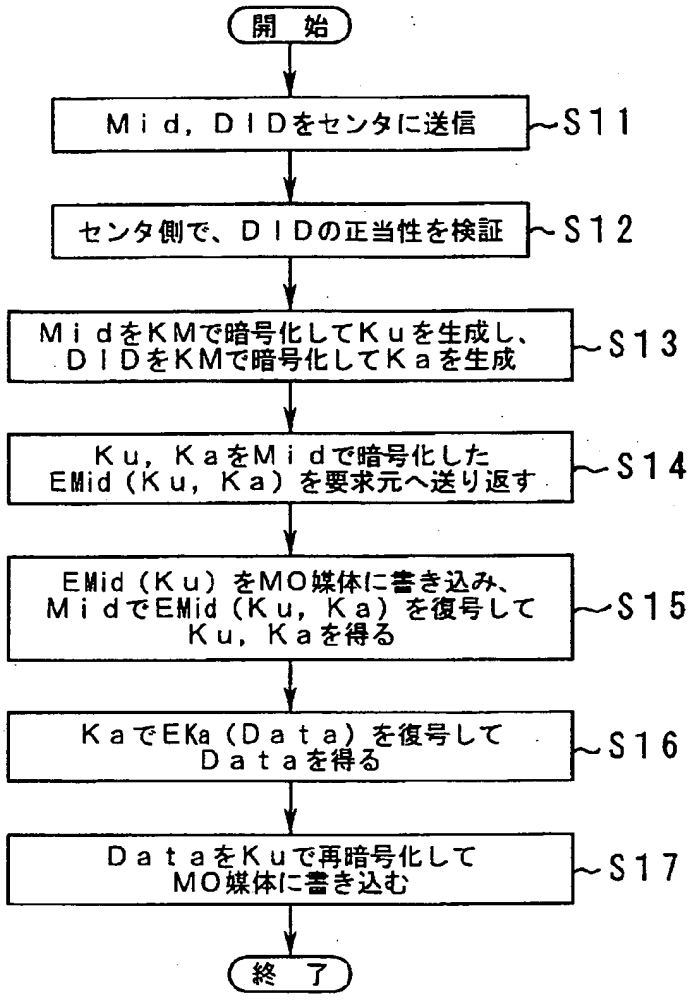
【図8】



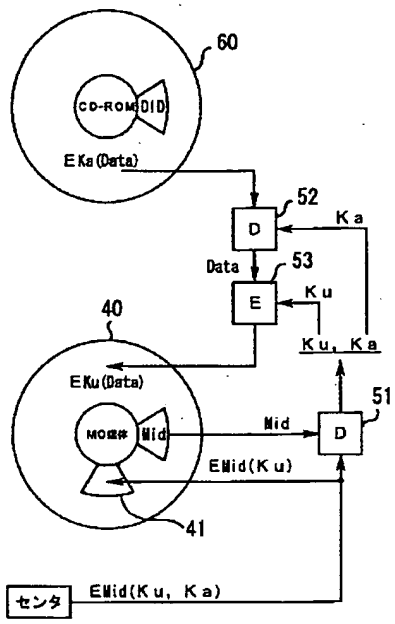
【図10】



【図7】


開　始
Ｍｉｄ，ＤＩＤをセンタに送信
S11
センタ側で、ＤＩＤの正当性を検証
S12
ＭｉｄをＫＭで暗号化してＫｕを生成し、
ＤＩＤをＫＭで暗号化してＫａを生成
S13
Ｋｕ，ＫａをＭｉｄで暗号化した
ＥＭｉｄ（Ｋｕ，Ｋａ）を要求元へ送り返す
S14
ＥＭｉｄ（Ｋｕ）をＭＯ媒体に書き込み、
ＭｉｄでＥＭｉｄ（Ｋｕ，Ｋａ）を復号して
Ｋｕ，Ｋａを得る
S15
ＫａでＥＫａ（Ｄａｔａ）を復号して
Ｄａｔａを得る
S16
ＤａｔａをＫｕで再暗号化して
ＭＯ媒体に書き込む
S17
終　了

【図9】


60
CD-ROM DID
EKa(Data)
52
D
Ka
Data
53
E
Ku
40
Ku，Ka
EKu(Data)
51
MO媒体
Mid
Mid
D
EMid(Ku)
41
センタ
EMid(Ku，Ka)